# Information Security Managers Group
# Tuesday, March 30, 2010 Meeting Minutes

***MEETING LOGISTICS (all meeting minutes are posted on the ISMG Sharepoint site:*** http://ent.sharepoint.mt.gov/groups/ism/default.aspx )

| | |
|---|---|
| When: | Last Tuesday of each month11:00 am – 12:00 pm |
| Who: | Agency CIO and/or Information Security Manager |
| Where: | Department of Labor and Industry First Floor Conference Room<br>Corner of Lockey and Sanders |
| Next Meeting: | Tentative - April 29, 2010 1:00 pm |

***PRESENT***

| | |
|---|---|
| MDT: | Kristi Antosh |
| DLI: | Lance Wetzel |
| DOC: | Larry Krause |
| OPI: | Jim Gietzen |
| DPHHS: | Chris Silvonen |
| DPHHS: | Jackie Thiel |
| DOA: | Larry Manchester |
| DOA: | Kevin Winegardner |
| DEQ: | Dan Chelini |
| DEQ: | Michael Jares |
| DNR: | Rick Bush |
| BPE: | Anneliese Warhank |

***PURPOSE***

The Information Security Managers Group has three primary purposes:

- Advise the State CIO on Information Risk Management Issues at the Statewide level
- Raise awareness while identifying communities of interest for EPP purposes
- Provide a forum for agency exchange of information

***AGENDA ITEMS***

- **Welcome and (re)introductions**

  The Group members introduced themselves around the table.

- **Update –ISMG Rules of Procedure – Approved by State CIO.**

  Rules are published on the ISMG Sharepoint site.

- **Update – Statewide Policy – Information Security Programs. Policy Published.**

  Effective Date is July 2012.

  Many ISM's are requesting staff to implement. Some agencies are working on developing their program plan to identify resource requirements. Some agencies think they may be found in non-compliance after 2012 policy effective date. There were differing opinions on this issue. It was noted however that there is a process available for requesting an exception to statewide policy that an agency is having difficulty complying with.

- **Update – DOA Prototyping Awareness, Training, and Education**
  - Larry Manchester gave an update on Awareness, Training, and Education progress. The prototyping of the first Tier of training continues. ISM's are encouraged to contact the

Enterprise Information System Security Bureau for more information. The ISM's message needs to drive the design of the presentation. Next level of detail is a course 6-8 weeks stepping through the NIST Risk Management Framework (RMF). The group agreed that a course on writing an Information Security Program Plan would be very valuable. The group decided that this would be the next training area, and that it is appropriate as the second step in the NIST RMF includes writing an Information Security Plan.

- **Short-Term Implementation Plan for the Risk Management Framework process**
    - Discussion. The group decided that this will be incorporated into training on Information Security Program Plan.

- **Guidance Documents – "System Authorization".**
    - This guideline has been retracted. It has been superseded by a revised publication in NIST, the recently finalized SP800-37 "Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach."

- **Rescinding of Legacy Statewide IT Policies**:
    - Discussion: A very lively discussion was had by the entire group. There will be continued discussion at Aprils meeting.

**Future Topics:**

Possible common EPP items:

- Risk Assessment Capabilities
- Planning of Program Implementation
- Staffing

***ACTION ITEMS***

- Schedule April 2010 ISMG meeting
    - Kevin Winegardner

***AGENDA ITEMS FOR NEXT MEETING***

- Update on next Awareness, Training and Education deliverable – Course on the NIST Risk Management Framework
    - Larry Manchester
- Legacy Statewide Information Security Policies – Continue Discussion
    - Group